04-10-00

jc712 U.S. PTO 04/07/00

Please type a plus sign (+) inside this box → +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	004814.P014
First Inventor or Application Identifier	Swain W. Porter
Title	METHOD AND APPARATUS FOR PROTECTIVELY OPERATING A DATA/INFORMATION PROCESSING DEVICE
Express Mail Label No.	EL034433935US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. ☒ Specification [*Total Pages* 20]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (*if filed*)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. ☒ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 6]

4. Oath or Declaration [*Total Pages* 3]
a. ☒ Newly executed (original copy)
b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 16 completed)
i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR §§ 1.63(d)(2) and 1.33(b).

5. ☐ Microfiche Computer Program *(Appendix)*

6. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ☐ Computer Readable Copy
b. ☐ Paper Copy (identical to computer copy)
c. ☐ Statement verifying identity of above copies

jc564 U.S. PTO 09/544492 04/07/00

NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

ACCOMPANYING APPLICATION PARTS

7. ☒ Assignment Papers (cover sheet & document(s))
8. ☐ 37 C.F.R. § 3.73(b) Statement *(when there is an assignee)* ☒ Power of Attorney
9. ☐ English Translation Document *(if applicable)*
10. ☐ Information Disclosure Statement (IDS)/PTO - 1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
13. ☒ *Small Entity Statement(s) ☐ Statement filed in prior application, Status still proper and desired
14. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
15. ☐ Other: .....

16. If a **CONTINUING APPLICATION**, *check appropriate box, and supply the requisite information below and in a preliminary amendment:*
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____
Prior application Information: Examiner _____ *Group/Art Unit:* _____
For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

☐ *Customer Number or Bar Code Label* *(Insert Customer No. or Attach bar code label here)* or ☒ *Correspondence address below*

Name	BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP				
Address	12400 Wilshire Boulevard, Seventh Floor				
City	Los Angeles	*State*	California	*Zip Code*	90025
Country	U.S.A.	*Telephone*	(503) 684-6200	*Fax*	(503) 684-3245

Name (Print/Type)	Aloysius T.C. AuYeung	Reg. No. 35,432	
Signature		*Date*	04/07/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

Applicant or Patentee: Swain W. Porter Attorney's
Serial or Patent No.: Docket No. 04814.P005
Filed or Issued:
For: **Method and Apparatus For Protectively Operating a Data/Information Processing Device**

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS
37 CFR 1.9 (f) and 1.27(c) - - SMALL BUSINESS CONCERN

I hereby declare that I am:

[XX] the owner of the small business concern identified below:
[_____] an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN: WILDSEED, INC.
ADDRESS OF CONCERN: 550 KIRKLAND WAY, N.E. SUITE 100, KIRKLAND, WA 98033

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.3-18, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees under Section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby certify that to the best of my knowledge and belief rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention entitled Method and Apparatus For Protectively Operating a Data/Information Processing Device by inventor(s) Swain W. Porter described in

[_____] the specification being filed herewith
[_____] application serial no. _____, filed _____
[_____] patent no. _____, issued _____

and I have reviewed the document that evidences the conveyance of those rights. That document

[_____] is being filed herewith.
[_____] was recorded in the Patent and Trademark Office on _____,19 __ at reel _____ and frame _____.

If the rights held by the above-identified small business concern are not exclusive, each individual, concern or organization having rights to the invention is listed below and **no rights to the invention are held by any person, other than the inventor, who could not qualify as a small business concern under 37 CFR 1.9(d) or by any concern which would not qualify as a small business concern under 347 CFR 1.9(d) or a non-profit organization under 37 CFR 1.9(e)**. NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

NAME: ______________________________
ADDRESS: ______________________________
[____] Individual [_____] Small Business Concern [_____] Non-Profit Organization
NAME: ______________________________
ADDRESS: ______________________________
[____] Individual [_____] Small Business Concern [_____] Non-Profit Organization

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING: SWAIN W. PORTER
TITLE OF PERSON OTHER THAN OWNER: ______________________________
ADDRESS OF PERSON SIGNING: ~~850~~ KIRKLAND WAY, N.E., SUITE 100, KIRKLAND, WA 98033
SIGNATURE: [signature] DATE: 4/7/00

Our Ref.: 004814.P014

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

Method And Apparatus For Protectively Operating A Data/Information Processing Device

Inventor(s): **Swain W. Porter**

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN, LLP
12400 Wilshire Boulevard, 7th Floor
Los Angeles, California 90025
(503) 684-6200

Method and Apparatus For Protectively Operating A Data/Information Processing Device

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of electronic data/information processing. More specifically, the present invention relates to methods and apparatuses for protectively operating data/information processing devices.

2. Background Information

The term "data/information processing devices" as used herein is intended to include all microprocessor based devices and/or systems, operated under the control of an operating system. Examples of these devices/systems include but are not limited to general as well as special purpose computing devices/systems, regardless of form factors, palm sized, laptops, desktops, rack mounted, and the like. Examples of special purpose computing devices include but are not limited to set-top boxes, wireless communication devices, and the like. The term "operating system" as used herein is intended to include all software provided to manage and facilitate application usage of hardware resources, however minimal the control and resource scope may be. Typical resource management functions of an "operating system" include task scheduling, memory management and the like. The term "task" as used herein is intended to include its common meaning of an executing instance of a program (a collection of programming instructions).

Ever since the early days of computing, computer systems have provided privilege protection to protect the system from being brought down by failures of

non-essential programs, such as application programs. The IBM 360 systems provided a supervisor mode and a user mode to segregate privileged system programs and unprivileged user programs. The Multics (Multiplexed Information and Computing Service) developed by Massachusetts Institute of Technology, in cooperation with others, employed a 64 ring approach, combining access node and a triple of ring numbers (r1, r2, r3). In U.S. Patent 4,177,510, issued to Appell et al., a hardware facilitated 4 ring approach is disclosed. Today, the Intel Architecture processors are known to provide a 4 ring hardware facilitated protection through the employment of memory segment descriptors and current task privilege level (CPL). However, partly because most of the other microprocessors remain having a two mode protection approach, the Windows® operating system, used in most Intel Architecture compatible processors, merely employ two of the four ring protection provided by the hardware. The kernel, virtual memory manager and various virtual device drivers (VxD) are executed in ring 0 (the most privileged level), while all other programs, including system services and so forth are executed out of ring 3 (the least privileged level). Rings 1 and 2 are not used.

The two levels of protection were reasonably adequate in the days when few programs are executed on most computer systems. Moreover, most of the computer systems operate by themselves, with few interactions from the outside world.

Advances in microprocessor, telecommunication and networking technology have dramatically expanded the applications of computing devices, and changed their operating environment. Today, most data/information processing systems are connected to private and/or public networks, such as the Internet, executing programs that are dynamically downloaded from a number of sources. Some

sources are trustworthy, and their programs tend to be well behaved, but others are not.

Accordingly, a need exists to improve the protection of data/information processing systems, especially those operating with a two privilege level protection scheme.

However, this need cannot be easily met, even in the case of systems using Intel Architecture processors and Windows operating system, where there are two unused privileged levels, as the system services and other trustworthy applications are confined to run at the least privileged level (ring 3). It would undermine the stability of the systems, as opposed to increasing its protection, if untrustworthy applications are confined to execute out of the more privileged ring 1 or ring 2. Relocating the operating system services and other trustworthy programs off the least privileged level (Ring 3) without hardware assistance would require major redesign of the operating system, and raises serious backward compatibility issues. Extending the hardware to have the processor support more privilege levels beyond 4 rings would require major redesign of the processor, as greater than 4 rings would require at least one extra bit be added to the current 2-bit representation. This would cause major redesign to the entire privilege level mechanism, including control register layouts, width of internal data lines, size of comparison circuitry and the like.

Thus, it is further desirable if the need can be met without requiring major processor and/or operating system re-design.

SUMMARY OF THE INVENTION

A privilege level re-mapping mechanism is provided to a processor to re-map privilege levels The re-mapping mechanism is placed in between the control registers and the privilege checking circuitry, to enable the re-mapping to be dynamically performed in real time prior to privilege checking. The novel dynamic re-mapping of privilege levels prior to privilege checking enables tasks to be executed with relative privilege level relationships that are different from what were nominally assigned to the tasks.

In one embodiment, complementary selection mechanism is also provided to enable the novel dynamic re-mapping to be conditionally performed.

BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

Figure 1 illustrates an overview of the present invention, in accordance with one embodiment;

Figures 2a-2b illustrate the privilege level re-mapper in further detail, in accordance with two embodiments;

Figures 3a-3b illustrate the privilege level re-mapper in further detail, in accordance with another two embodiments;

Figure 4 illustrates another overview of the present invention, in accordance with another embodiment;

Figure 5 illustrates an example application of the present invention; and

Figure 6 illustrates an example system incorporated with the processor of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention. For purposes of explanation, specific numbers, materials and configurations are set forth in order to provide a thorough understanding of the present invention. However, it will also be apparent to one skilled in the art that the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Parts of the description will be presented using terms such as privilege levels, control registers, and so forth, commonly employed by those skilled in the art to convey the substance of their work to others skilled in the art. Parts of the description will be presented in terms of operations performed by a computer system, using terms such as privilege checks, and so forth. As well understood by those skilled in the art, these quantities and operations take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, and otherwise manipulated through mechanical and electrical components of a digital system; and the term digital system include general purpose as well as special purpose data processing machines, systems, and the like, that are standalone, adjunct or embedded.

Various operations will be described as multiple discrete steps performed in turn in a manner that is most helpful in understanding the present invention, however, the order of description should not be construed as to imply that these operations are necessarily order dependent, in particular, the order the steps are presented.

Furthermore, the phrase "in one embodiment" will be used repeatedly, however the phrase does not necessarily refer to the same embodiment, although it may.

Referring now to **Figure 1**, wherein an overview of the present invention in accordance with one embodiment is shown. As illustrated, in accordance with the present invention, a task current privilege level (CPL) remapper **104** that re-maps a task's CPL from one assigned level to another is provided to processor **100**. Task CPL remapper **104** is strategically placed in between task register **102** (a control register where task CPL is stored) and privilege level checking mechanism **106** to enable the re-mapping to be dynamically performed in real time prior to privilege checking during execution. The novel dynamic re-mapping of privilege levels prior to privilege checking advantageously enables tasks to be executed with relative privilege level relationships that are different from what were nominally assigned to the tasks.

Except for the teachings of the present invention incorporated, processor **100** is otherwise intended to represent a broad range of processors known in the art. As will be readily apparent from the descriptions to follow, while **Fig. 1** specifically illustrates the task register where a task's current privilege level, the present invention applies to privilege level in general, and may be practiced to dynamically alter the relative privilege relationship between memory segments, selectors, descriptors and the like. For ease of understanding, the remaining description will nevertheless continue to primarily refer to the task's CPL. Privilege checking mechanism **106** is intended to represent a broad range of privilege checking mechanisms or circuitry known in the art. It may enforce any one of a number privilege rules, as well as enforcing these rules in any one of a number of implementation manner. Neither the privilege rules being enforced nor the manner

they are enforced are of particular relevance to the practice of the present invention. In fact, a major advantage of the present invention is the ability to introduce a new order of privilege relationship without requiring major re-design to the fundamental privilege protection mechanism of a processor nor the operating system that uses the processor.

Figures 2a-2b illustrate task CPL re-mapper **104** in further detail, in accordance with two embodiments. **Fig. 2a** illustrates a basic embodiment, where a new control register **202** is used to re-map a task's CPL. As illustrated, the re-targeted privilege levels are stored in register **202**, and they are selectively accessed and retrieved using the task CPL read out of task register **102** as an offset into register **202**. As a result, a task having a CPL of "0" or "1" will retain the "0" or "1" CPL, whereas a task with a CPL of "2" will be re-mapped to a CPL of "3", and a task with a CPL of "3" will be re-mapped to a CPL of "2". Accordingly, the desired privilege level re-mapping, and relative privlege relationship re-ordering is achieved in accordance with the stored scheme.

Fig. 2b illustrates a more elaborate embodiment, where a memory storage array **204** is used to re-map a task's CPL. As illustrated, multiple sets of re-targeted privilege levels are stored in array **204**, and they are selectively accessed and retrieved using the task CPL read out of task register **102** as a row pointer into array **204**, in conjunction with a configuration signal serving as a column pointer into array **204**. As a result, a task having a CPL of "0", "1", "2" or "3" may be re-mapped to "0", "1", "3" and "2" respectively as before, if the set stored in column 1 is used, or to "1", "0", "3" and "2" respectively, if the set stored in column 4 is used instead. Accordingly, the desired privilege level re-mapping, and relative privilege relationship re-ordering is achieved in accordance with one of the stored schemes.

The re-targeted privilege levels representing a re-mapping scheme may be "hard coded" into register **202** or array **204**, or it may be loaded at power-on or reset as part of the initialization process. The configuration signal may be driven e.g. off a programmable configuration register (not shown).

Thus, it can be seen from the embodiments of **Fig. 2a-2b**, the present invention may be practiced with a simple pre-determined re-mapping scheme or with a re-mapping scheme to be configurably determined from a rich or full set of all possible re-mappings.

Figures 3a-3b illustrate task CPL re-mapper **104** in further detail, in accordance with another two embodiments. **Fig. 3a** achieves the same re-mapping as the embodiment of **Fig. 2b** if the set of re-targeted privilege levels stored in column 4 are used. Except, under **Fig. 3a**, the re-mapping is achieved through a combinatorial circuit element, XOR gate **302**. More specifically, the lower order bit of a task's CPL is XOR'd with the value "0" to alter it, while the higher order bit is retained. Effectively, a task with CPL "00", "01", "10" and "11" (0, 1, 2, 3 in decimal) will be re-mapped to "01", "00", "11" and "10" (1, 0, 3, 2 in decimal).

Fig. 3b may achieve a number of re-mappings possible under the earlier described embodiments. Except, under **Fig. 3b**, the re-mapping is also achieved through a combinatorial circuit element, XOR gate **302**. In addition to XOR gate **302**, the embodiment of **Fig. 3b** is also provided with selector **304** to allow the selective retaining of the original lower bit or the employment of the altered lower bit. Selector **304** selects either the original lower bit or the altered lower bit in accordance with a configuration signal. The original lower bit (or the altered lower bit) may be selected with the configuration signal equals "0" or "1". The manner of selection is immaterial. Thus, if configuration signal always selects the original

lower bit, re-mapping is effectively disabled. On the other hand, if configuration signal is conditionally driven to select the altered lower bit, depending on whether the lower bit is "1" or "0", it achieves the same re-mapping offered by the embodiment of **Fig. 2b** employing column 1 (which is the same as the embodiment of **Fig. 2a**), or the re-mapping offered by the embodiment of **Fig. 2b** employing column 3. Finally, if configuration signal always selects the original altered lower bit, the embodiment of **Fig. 3b** is effectively the same as the embodiment of **Fig. 3a**.

Similarly, configuration signal may be driven from a programmable configuration register, or outputs of other combinatorial circuits. Thus, it can be seen that various re-mapping may also be achieved through combinatorial circuits. The embodiments of **Fig. 3a-3b** are kept simple for ease of understanding. However, those skilled in the art will be able to extend from these embodiments to allow even more flexible re-mapping of various kinds.

Figure 4 illustrates another overview of the present invention, in accordance with another embodiment. The embodiment of **Fig. 4** is essentially that of the embodiment of **Fig. 1**, except for the provision of selector **402** to allow the re-mapping to be selectively enabled and disabled. In other words, the inclusion of selector **402** enables the present invention to be configurably included or excluded.

Figure 5 illustrates an example application of the present invention. As illustrated, in this example application, the kernel, the virtual device driver and the memory manager of an operating system are nominally attributed with task CPL "0", enabling them to execute in privilege ring 0, whereas other operating system services, as well as "trustworthy" applications are nominally attributed with task CPL "3", confining them to execute in privilege ring 3. Untrustworthy applications, such

as Internet applications, are nominally attributed with task CPL "2', enabling them to execute in the more privileged ring 2.

However, employing the present invention, the privilege levels are dynamically re-mapped, enabling the relocation of the operating system services and trustworthy applications to the more privileged ring 2, and confining the untrustworthy Internet application to the least privileged ring 3 instead.

What constitutes trustworthiness is application dependent. Their demarcation is immaterial for the practice of the present invention. Further, the term "privilege ring" or "ring" as used herein is intended to include its conventional meaning that a program afforded a more inner privilege ring typically has privileges inclusive that of another program afforded a more outer privilege ring.

Thus, it can be seen under the present invention, a class of lesser privileged tasks can be carved out of the existing least privileged tasks. The new least privileged tasks will first be nominally given a more privileged level. But, at execution time, the privilege levels of the residual former least privileged tasks and the new least privileged tasks are re-mapped (prior to privilege checking), and re-ordered to the desired relative privilege relationship. Likewise, the same may be performed at the other end of the privilege spectrum. That is, a class of more privileged tasks can be carved out of the existing most privileged tasks. The new more privileged tasks will first be nominally given a lesser privilege level. But, at execution time, the privilege levels of the residual former most privileged tasks and the new more privileged tasks are re-mapped (prior to privilege checking), and re-ordered to the desired relative privilege relationship.

Referring now to **Figure 6**, wherein a block diagram illustrating an example system incorporated with the teachings of the present invention is shown. System

600 is intended to represent a broad range of digital systems or devices known in the art, including but not limited to computer systems of all form factors (from palm-sized, to laptop, desktop and racked mounted servers), telecommunication devices such as wireline or wireless telephones, or entertainment devices such as set top devices, and the like. As shown, example system **600** includes processor **602**, system memory **604** coupled to each other via "bus" **612**. Coupled also to "bus" **612** are non-volatile storage **606**, input/output device **608** and communication interface **610**.

Processor **602** may be the processor of **Fig. 1**, **Fig. 4**, and other equivalents. Each of the other enumerated elements is intended to represent a wide range of the respective devices/elements known in the art. For example, system memory **604** may be SDRAM, DRAM and the like, from semiconductor manufacturers such as Micron Technology of Boise, Idaho. Bus **612** may be a single bus or a multiple bus implementation. In other words, bus **612** may include multiple buses of identical or different kinds properly bridged, such as Local Bus, VESA, ISA, EISA, PCI and the like. Non-volatile storage **606** may be disk drives or CDROMs from manufacturers such as Seagate Technology of Santa Cruz of CA, and the like. Input/Output devices **608** may include input devices, such as keypads, key boards, or cursor control devices like a mouse, a track ball and so forth, from vendors such as Logictech of Milpitas, CA, and output devices like display devices such as LCD displays, flat panel displays or monitors of any types, from vendors such as Viewsonic of Walnut, CA. Communication interface **610** may be a wireless interface, or a wireline interface, such as modem interface, an ISDN adapter, a DSL interface, an Ethernet or Token ring network interface and the like, from vendors such as 3COM of San Jose, CA.

Thus, a method and apparatuses for protectively operating a data/information processing system has been described. While the present invention has been described in terms of the above illustrated embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described. The present invention can be practiced with modification and alteration within the spirit and scope of the appended claims. The description is thus to be regarded as illustrative instead of restrictive on the present invention.

CLAIMS

What is claimed is:

1. A processor comprising:

a control register to store a task privilege level for a task; and

a privilege remapper coupled to the control register to dynamically remap the stored task privilege level.

2. The processor of claim 1, wherein the privilege remapper comprises a register to store a plurality of remapped task privilege levels to be accessed using the stored task privilege level prior to runtime privilege checking.

3. The processor of claim 1, wherein the privilege remapper comprises a storage array to store a plurality of set of remapped task privilege levels to be accessed using a configuration value and the stored task privilege level prior to runtime privilege checking.

4. The processor of claim 1, wherein the privilege remapper comprises one or more logical elements to logically alter one or more bits of the stored privilege level prior to runtime privilege checking.

5. The processor of claim 1, wherein the privilege remapper further comprises at least one selector coupled to at least one of the one or more logical elements to effectuate conditional performance of said logically alteration for at least one bit of the stored privilege level prior to runtime privilege checking.

6. The processor of claim 1, wherein the processor further comprises at least one selector coupled to the control register and the privilege remapper to effectuate conditional performance of said remapping of the stored task privilege level prior to runtime privilege checking.

7. A method comprising:

storing a first task privilege level for a task; and

dynamically remapping the first task privilege level to a second task privilege level prior to runtime privilege checking to effectuate a different execution privilege level for the task.

8. The method of claim 7, wherein said dynamic remapping comprises accessing a register to retrieve a selected one of a plurality of remapped task privilege levels stored in said register, using the stored first task privilege level, prior to runtime privilege checking.

9. The method of claim 7, wherein said dynamic remapping comprises accessing a storage array to retrieve a selected one of a plurality of remapped task privilege levels stored in said storage array in a set-wise manner, using a configuration value and the stored first task privilege level, prior to runtime privilege checking.

10. The method of claim 7, wherein said dynamic remapping comprises logically altering one or more bits of the stored first task privilege level, prior to runtime privilege checking.

11. The method of claim 10, wherein said altering being conditionally performed.

12. The method of claim 1, wherein said dynamic remapping being conditionally performed.

13. In a processor having a 4-ring privilege protection scheme, where tasks attributed with a lower ring privilege level is more privileged than tasks attributed with a higher ring privilege level, a method comprising:

attributing a ring-2 privilege level to a first task, nominally giving said first task more privilege than a second plurality of tasks which are attributed with a ring-3 privilege level; and

dynamically remapping each ring-2 privilege level to a ring-3 privilege level, and each ring-3 privilege level to a ring-2 privilege level prior to runtime privilege checking to cause said first task to execute in fact with less privileges than said second plurality of tasks.

14. The method of claim 13, wherein said first task is associated with an Internet application.

15. The method of claim 13, wherein said second plurality of tasks are associated with an operating system.

16. A method comprising:

attributing a first privilege level to a first collection of programming instructions, said first privilege level being different from a second privilege level

assigned to a second collection of programming instructions, resulting in said first collection of programming instructions to execute with a first relative privilege relationship to said second collection of programming instructions at execution time; and

dynamically remapping said first privilege level to a third privilege level prior to runtime privilege checking to cause the first collection of programming instructions to execute with a second different relative privilege relationship to said second collection of programming instructions.

17. The method of claim 16, wherein said second and third privilege levels are the same privilege level, and said method further comprises dynamically remapping said second privilege level of said second collection of programming instructions to a fourth privilege level prior to runtime privilege checking.

18. The method of claim 17, wherein said first and fourth privilege levels are the same privilege level.

19. A method comprising:

attributing a first more privileged privilege level to a first subset of least privileged tasks attributed with a least privileged privilege level; and

dynamically remapping said first more privileged privilege level attributed to said first subset of least privileged tasks to said least privileged privilege level, and remapping said least privileged privilege level attributed to residual ones of said least privileged tasks prior to runtime privilege checking to cause said first subset of least privileged tasks to execute with lesser privileges than said residual ones of the least privileged tasks.

20. The method of claim 21, wherein said least privileged privilege level of said residual ones of said least privileged tasks are remapped to said first more privileged privilege level.

21. A method comprising:

attributing a first lesser privileged privilege level to a first subset of most privileged tasks attributed with a most privileged privilege level; and

dynamically remapping said first lesser privileged privilege level attributed to said first subset of most privileged tasks to said most privileged privilege level, and remapping said most privileged privilege level attributed to residual ones of said most privileged tasks prior to runtime privilege checking to cause said residual ones of the most privileged tasks to execute with lesser privileges than said first subset of most privileged tasks.

22. The method of claim 21, wherein said most privileged privilege level of said residual ones of said most privileged tasks are remapped to said first lesser privileged privilege level.

23. A processor comprising:

a control register to store a privilege level; and

a privilege remapper coupled to the control register to dynamically remap the stored privilege level prior to runtime privilege checking.

24. The processor of claim 23, wherein the processor further comprises at least one selector coupled to the control register and the privilege remapper to effectuate

conditional performance of said remapping of the stored privilege level prior to runtime privilege checking.

25. An apparatus comprising:

a control register to store a privilege level; and

a privilege remapper coupled to the control register to dynamically remap the stored privilege level prior to runtime privilege checking.

26. The apparatus of claim 25, wherein the apparatus further comprises at least one selector coupled to the control register and the privilege remapper to effectuate conditional performance of said remapping of the stored privilege level prior to runtime privilege checking.

ABSTRACT OF THE DISCLOSURE

A privilege level re-mapping mechanism is provided to a processor to re-map privilege levels. The re-mapping mechanism is placed in between the control registers and the privilege checking circuitry, to enable the re-mapping to be dynamically performed in real time prior to privilege checking. The novel dynamic re-mapping of privilege levels prior to privilege checking enables tasks to be executed with relative privilege level relationships that are different from what were nominally assigned to the tasks. In one embodiment, complementary selection mechanism is also provided to enable the novel dynamic re-mapping to be conditionally performed.

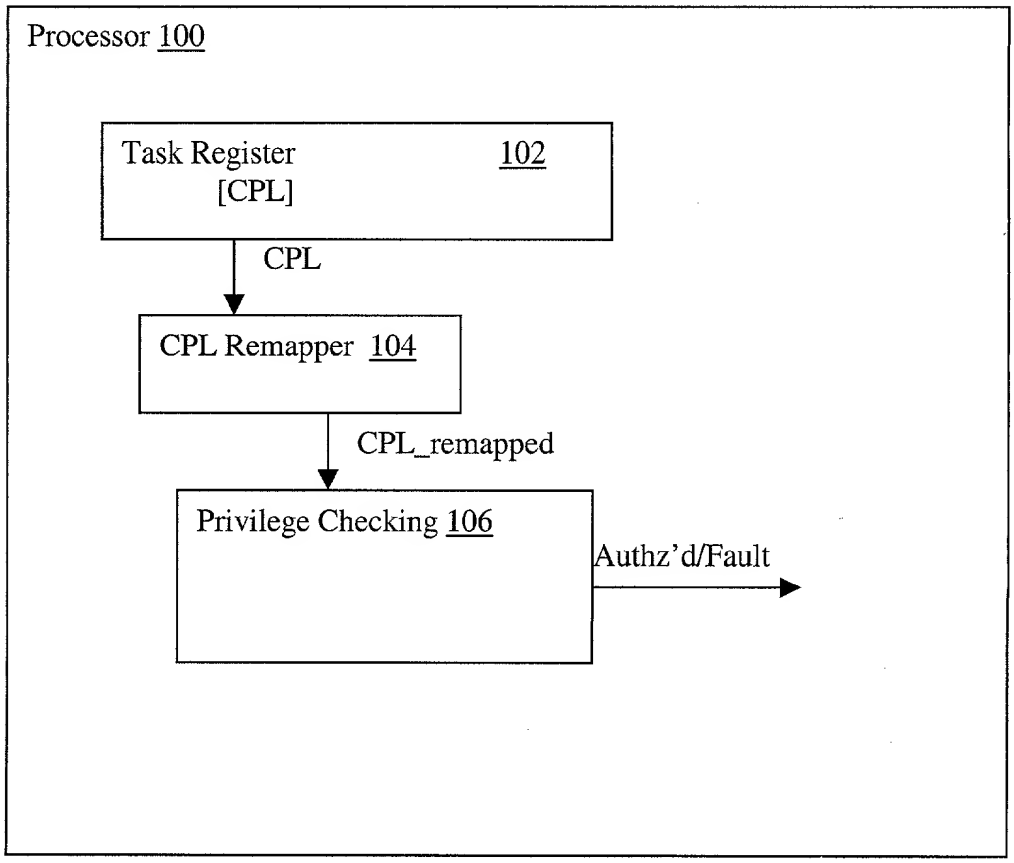
Processor 100
Task Register 102
[CPL]
CPL
CPL Remapper 104
CPL_remapped
Privilege Checking 106
Authz'd/Fault

Figure 1

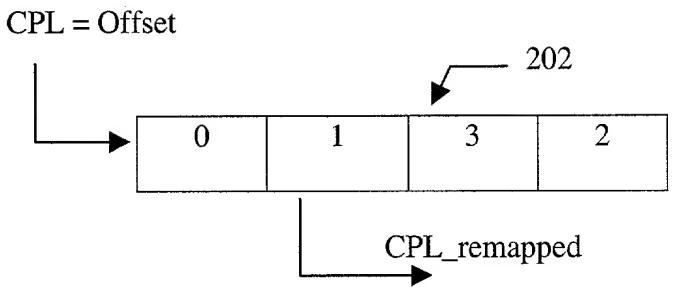
CPL = Offset
202
0
1
3
2
CPL_remapped

Fig. 2a

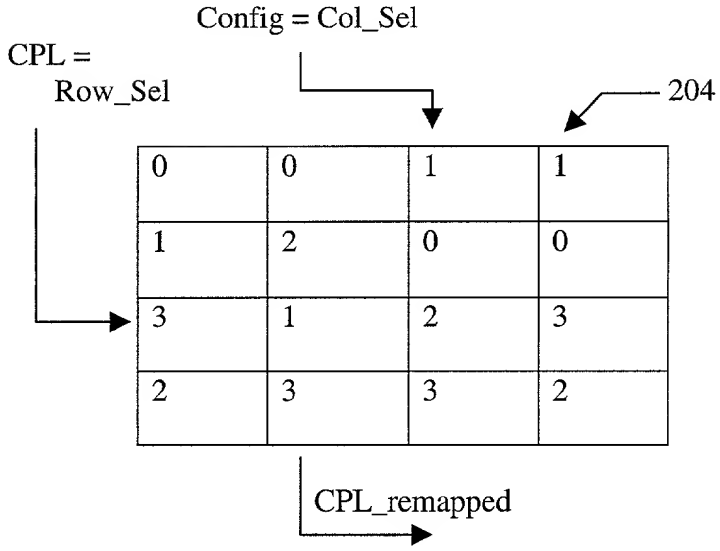
Config = Col_Sel
CPL =
Row_Sel
204
0
0
1
1
1
2
0
0
3
1
2
3
2
3
3
2
CPL_remapped

Fig. 2b

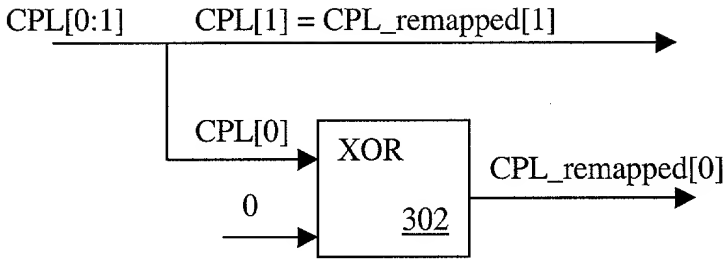
CPL[0:1]
CPL[1] = CPL_remapped[1]
CPL[0]
XOR
CPL_remapped[0]
0
302

Fig. 3a

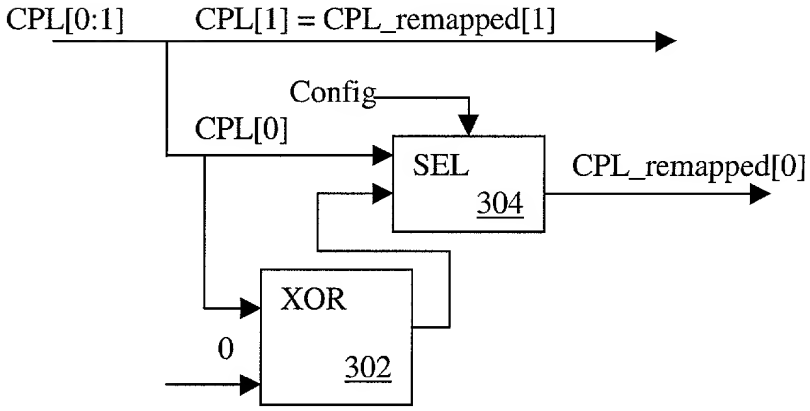
CPL[0:1]
CPL[1] = CPL_remapped[1]
Config
CPL[0]
SEL
CPL_remapped[0]
304
XOR
0
302

Fig. 3b

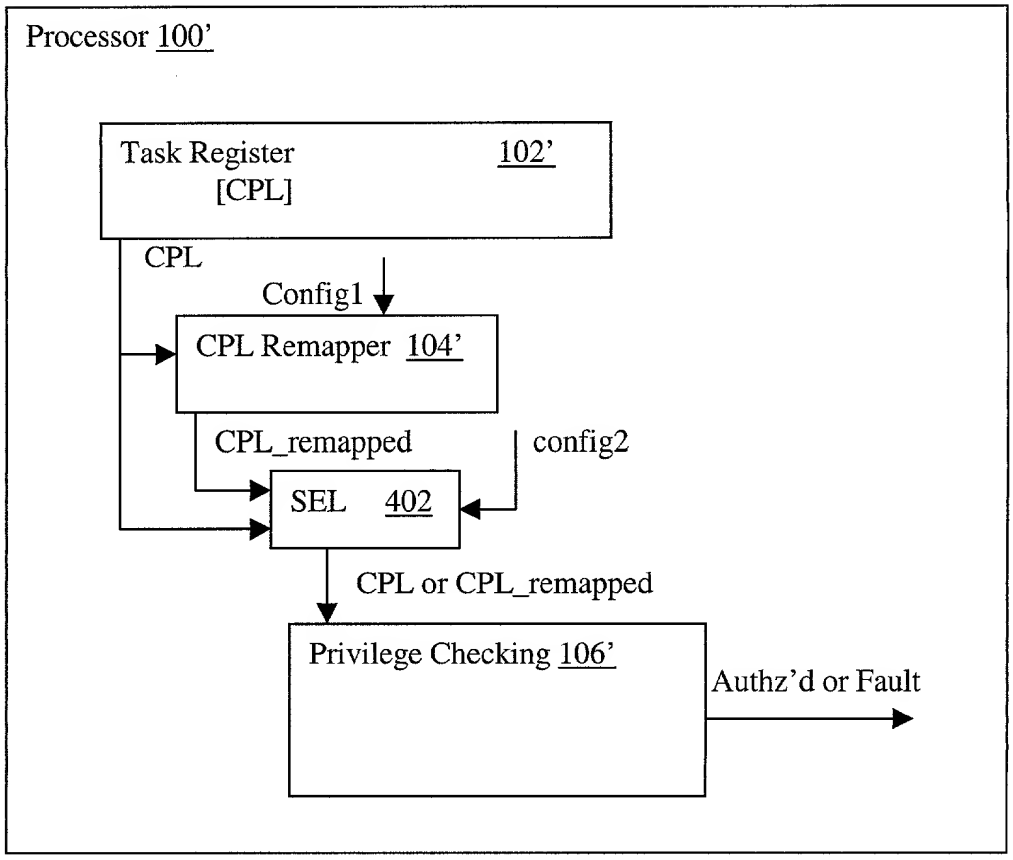
Processor 100'
Task Register 102'
[CPL]
CPL
Config1
CPL Remapper 104'
CPL_remapped
config2
SEL 402
CPL or CPL_remapped
Privilege Checking 106'
Authz'd or Fault

Fig. 4

500

Nominal Assignment

Ring 0 Memory Management, Kernel Virtual Device Drivers
Ring 1
Ring 2 Internet Applications
Ring 3 OS System Services & Other Applications

Actual Privilege Relationship Upon Re-mapping

Ring 0 Memory Management, Kernel Virtual Device Drivers
Ring 1
Ring 2 …OS System Services & Other Applications
Ring 3 …Internet Applications

Fig. 5

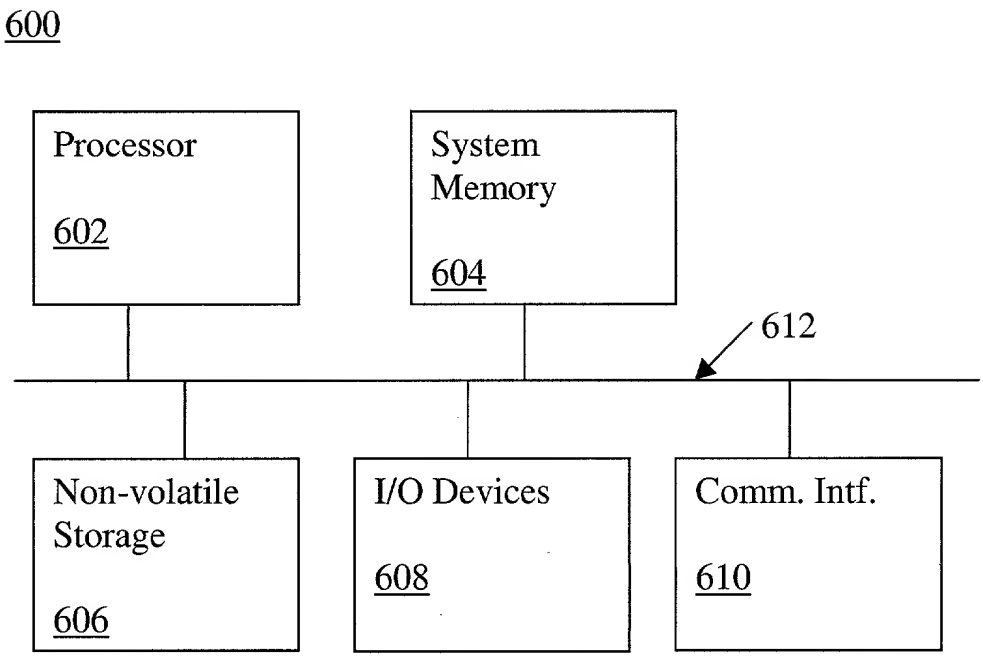
600
Processor
602
System
Memory
604
612
Non-volatile
Storage
606
I/O Devices
608
Comm. Intf.
610

Figure 6

Attorney's Docket No.: 04184.P014 PATENT

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD AND APPARATUS FOR PROTECTIVELY OPERATING A DATA/INFORMATION PROCESSING DEVICE

the specification of which

XX is attached hereto.
____ was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s) — Priority Claimed

(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below

(Application Number)	Filing Date
(Application Number)	Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Number)	Filing Date	(Status -- patented, pending, abandoned)
(Application Number)	Filing Date	(Status -- patented, pending, abandoned)

I hereby appoint Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; Amy M. Armstrong, Reg. No. 42,265; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Kent M. Chen, Reg. No. 39,630; Lawrence M. Cho, Reg. No. 39,942; Yong S. Choi, Reg. No. P43,324; Thomas M. Coester, Reg. No. 39,637; Roland B. Cortes, Reg. No. 39,152; Barbara Bokanov Courtney, Reg. No. 42,442; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Tarek N. Fahmi, Reg. No. 41,402; James Y. Go, Reg. No. 40,621; Richard Leon Gregory, Jr., Reg. No. 42,607; Dinu Gruia, Reg. No. P42,996; David R. Halvorson, Reg. No. 33,395; Thomas A. Hassing, Reg. No. 36,159; Phuong-Quan Hoang, Reg. No. 41,839; Willmore F. Holbrow III, Reg. No. P41,845; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; Dag H. Johansen, Reg. No. 36,172; William W. Kidd, Reg. No. 31,772; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. 42,004; Chun M. Ng, Reg. No. 36,878; Thinh V. Nguyen, Reg. No. 42,034; Kimberley G. Nobles, Reg. No. 38,255; Michael A. Proksch, Reg. No. 43,021; Babak Redjaian, Reg. No. 42,096; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Anand Sethuraman, Reg. No. P43,351; Charles E. Shemwell, Reg. No. 40,171; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; George G. C. Tseng, Reg. No. 41,355; Lester J. Vincent, Reg. No. 31,460; John Patrick Ward, Reg. No. 40,216; Stephen Warhola, Reg. No. 43,237; Charles T. J. Weigell, Reg. No. 43,398; Steven D. Yates, Reg. No. 42,242; Ben J. Yorks, Reg. No. 33,609; and Norman Zafman, Reg. No. 26,250; my attorneys, and James A. Henry, Reg. No. 41,064; Daniel E. Ovanezian, Reg. No. 41,236; Glenn E. Von Tersch, Reg. No. 41,364;; and Chad R. Walsh, Reg. No. 43,235; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to **Aloysius T.C. AuYeung**, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct telephone calls to **Aloysius T.C. AuYeung**, (503) 684-6200.

(Name of Attorney or Agent)

(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor SWAIN W. PORTER

Inventor's Signature Swain W Porter Date 4/7/00

Residence Kirkland, Washington (City, State) Citizenship USA (Country)

Post Office Address 12511 89th Ct. NE
Kirkland, Washington 98034

Full Name of Second/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

Post Office Address _____

Full Name of Third/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

Post Office Address _____

Full Name of Fourth/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

Post Office Address _____

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclosure all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.